BLOCKCHAIN SECURITY IN THE QUANTUM AGE

2024/03/18

ATH - ALL TIME HIGH

Bitcoin Hits $68K ATH, Sparking Rally in AI Altcoins

Published on March 5, 2024 01:53
By **Arezki Amiri**

HOME » CRYPTO NEWS » BITCOIN JUST BROKE THE ALL-TIME HIGH RECORDED IN DECEMBER 2017

Bitcoin Just Broke The All-Time High Recorded In December 2017

Author: George Georgiev • Last Updated Nov 30, 2020 @ 14:53

Following three long years of waiting, Bitcoin price has finally breached the all-time high record set all the way back in December 2017.

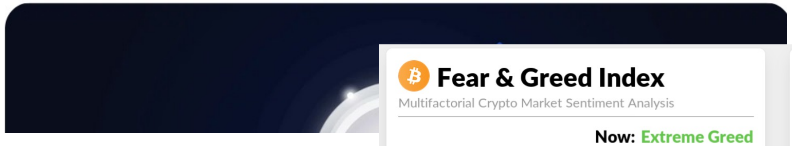
Bitcoin (BTC) Price To Hit New ATH in Next Few Hours, What To Expect Next?

Author: Elena R Mar 5, 2024 7:20

Ethereum Price Prediction: Will ETH Price Aim to Touch New ATH of $5000 in 2024?

Unlock the potential as Ethereum eyes a promising $5000 target.

4 Mar 2024 | 11 min read



ATH - ALL TIME HYPE

FORBES > INNOVATION

Quantum Computers Could Make Today's Encryption Defenseless

Markus Pflitsch Forbes Councils Member
Forbes Technology Council
COUNCIL POST | Membership (Fee-Based)

May 4, 2023, 08:30am EDT

Markus Pflitsch, CEO and Founder of Terra Quantum, is a dedicated quantum physicist, senior financial executive and deep tech entrepreneur.

Technology

Quantum computers can break major encryption method, researchers claim

It has long been known that one day quantum computers will probably be able to crack the RSA encryption method we use to keep data safe, but a team of researchers is now claiming it is already possible, while others say the results require more scrutiny

By Matthew Sparkes

5 January 2023

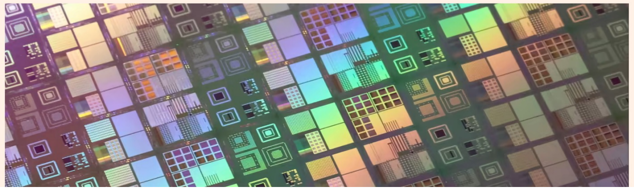
FINANCIAL TIMES

US COMPANIES TECH MARKETS CLIMATE OPINION WORK & CAREERS LIFE & ARTS HTSI

Quantum technologies + Add to myFT

Chinese researchers claim to find way to break encryption using quantum computers

Experts assess whether method outlined in scientific paper could be a sooner-than-expected turning point in the technology



INTERESTING ENGINEERING Subscribe | Sign In

IBM's quantum leap: A 100,000-Qubit supercomputer on the horizon

IBM has unveiled its ambitious plan to construct a groundbreaking 100,000-qubit quantum computer within the next decade.

INNOVATI

ZDNET

Home / Tech / Security

White House: Quantum computers could crack encryption, so here's what we need to do

Whoever wins the quantum computing race could undermine national security systems and the nation.

COINTELEGRAPH
The future of money

News Markets Magazine People Cryptopedia Research Video

ZHIYUAN SUN JAN 05, 2023

Quantum computers may soon breach blockchain cryptography: Report

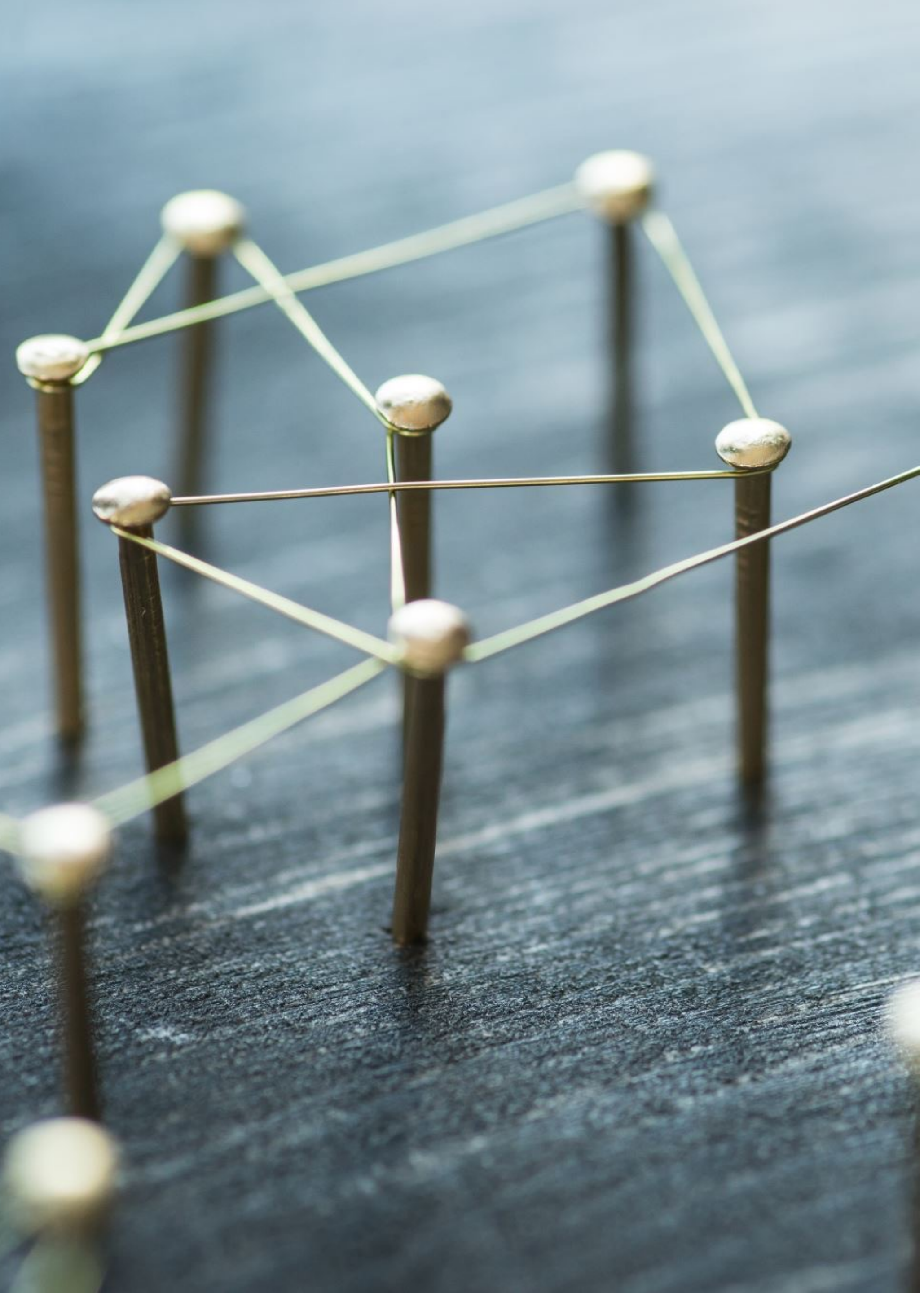
Cryptography experts are somewhat skeptical of the technique's scalability but aren't ruling out the possibility of success either.

14928 Total views 123 Total shares Listen to article 3:50

ATH – ALL TIME HORROR?

ARE CRYPTOS DOOMED!? 😱

Let’s find out!



WHO AM I

- Gottfried Szing
- Freelancer for 20+ years
- Business analyst / Architect / Requirements engineer
- Co-organizer of meetups
    - Microservices, Reactive and Distributed Systems
    - DDD Vienna
    - DLT Austria
    - Business Analysis Vienna (rebooting)

gottfriedszing

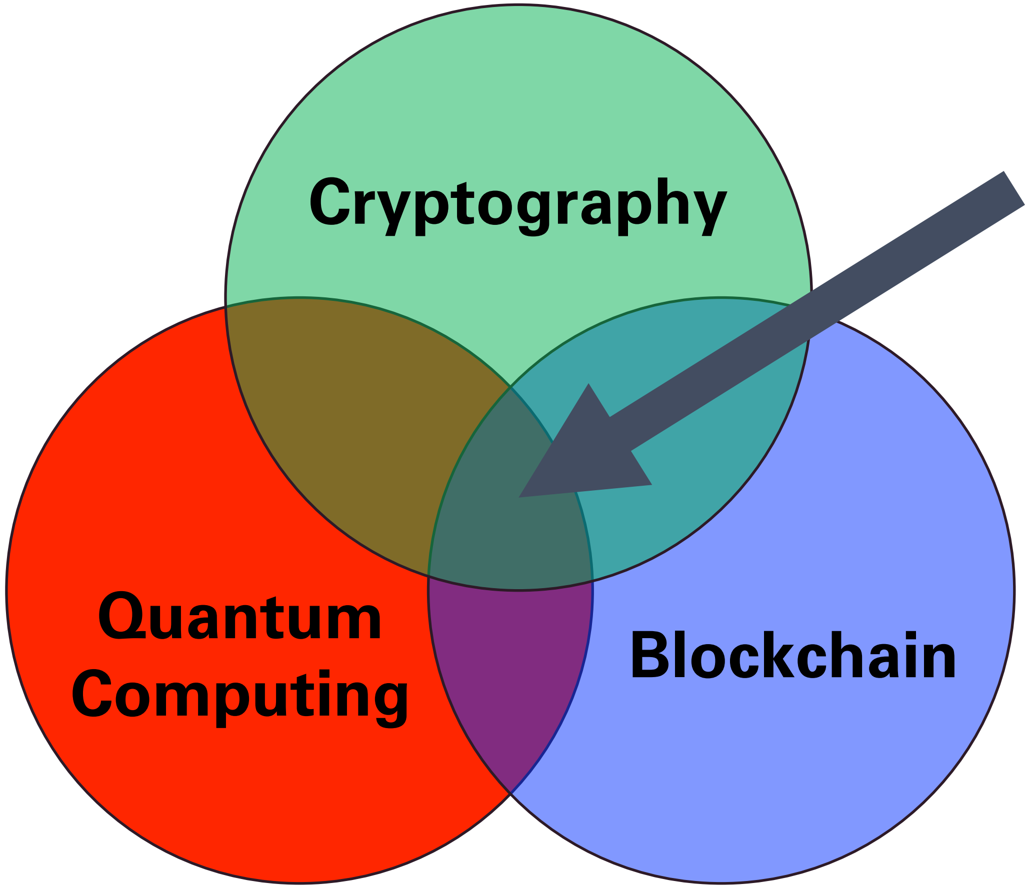
gottfried@szing.eu


https://commons.wikimedia.org/wiki/File:Snorkeler_dive_into_a_shallow_river.jpg

DISCLAIMER

- No financial advice!
- No investment advice!
- No guarantees!
- No responsibility!
- No deep-dive!

DYOR!



AGENDA

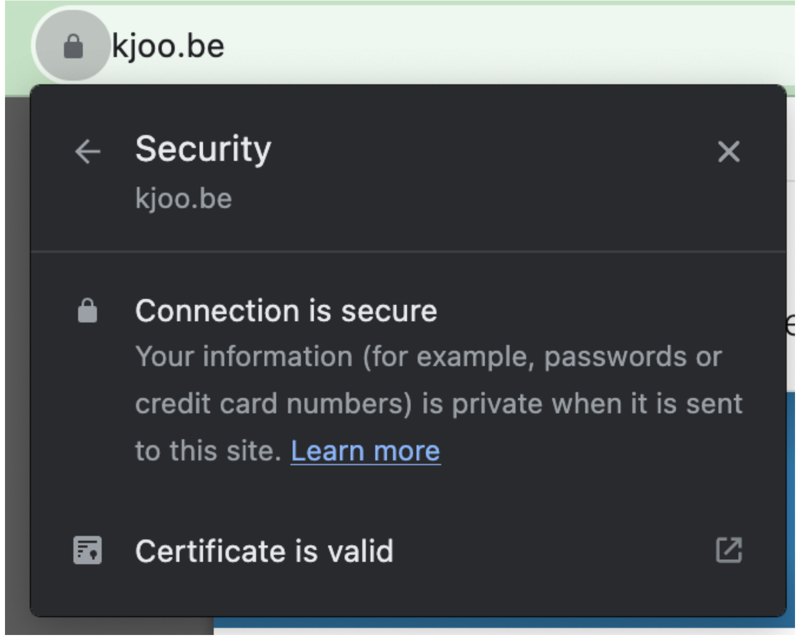
- What is Cryptography?
- What is a Blockchain?
- What is Quantum Computing?

- Attacks to Blockchain?

- Quantum-first Blockchain and
- Current state on Quantum Resistance

WHAT IS CRYPTOGRAPHY?

OBJECTIVES OF CRYPTOGRAPHY



- CIA Triad
  - **C**onfidentiality
    - Protects confidentiality of information (MITM)
    - Only authorized persons have access to information
    - Assures that the sender or receiver is the right one
  - **I**ntegrity
    - Ensures integrity of your data
    - Enables non-repudiation
    - Authenticity
  - **A**vailability
    - Securing systems
    - Systems, networks, and applications must be functioning

COMPONENTS OF A CRYPTOSYSTEM

Modern Cryptography provides following methods

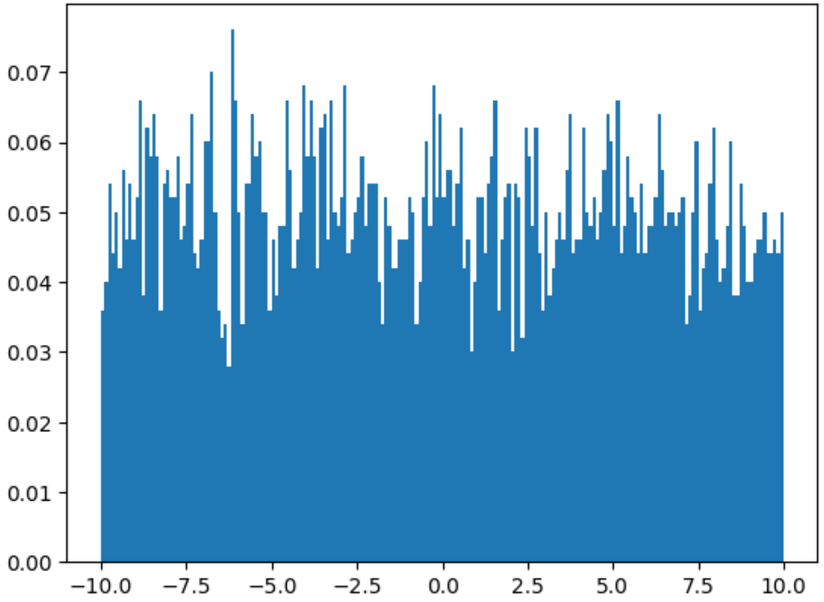
1. Key generation
2. Symmetric cryptography
3. Asymmetric cryptography
4. Cryptographic hash functions
5. Digital signatures

Items 2–3: Confidentiality

Items 4–5: Integrity

KEY GENERATION

- Keys are needed for cryptography
  - Randomly
  - Uniformly
  - Unique

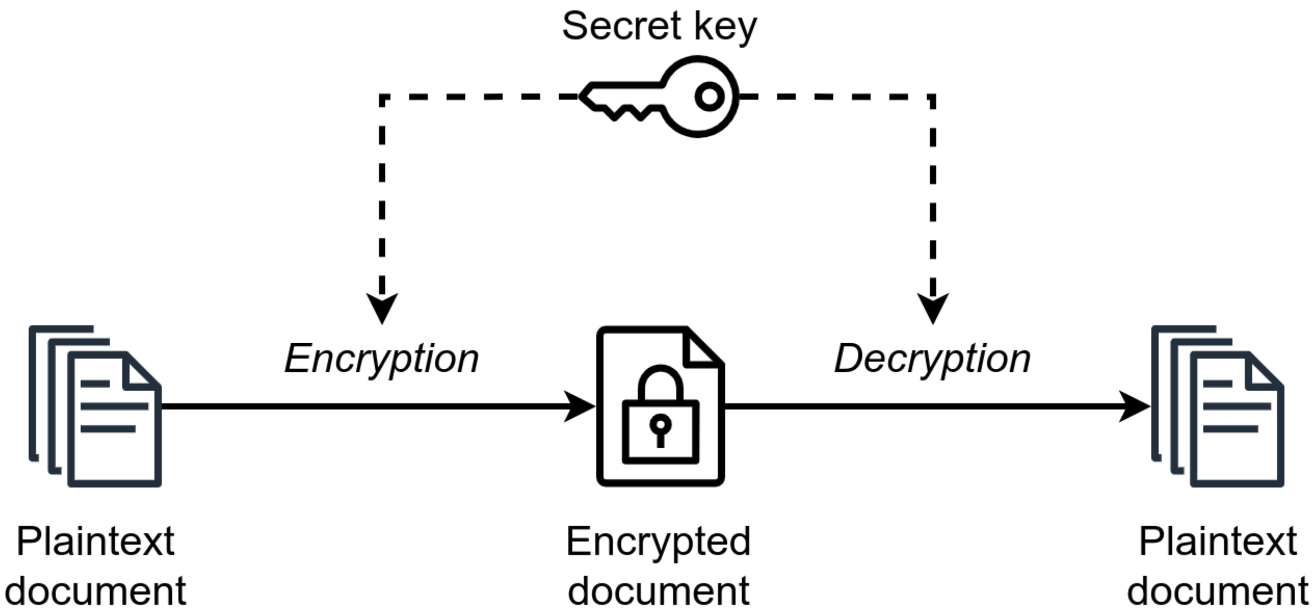


- Examples
  - Pseudo Random Number Generator (PRNG)
  - Adding entropy by hardware, network traffic, Lavarand,…

https://blog.cloudflare.com/lavarand-in-production-the-nitty-gritty-technical-details

SYMMETRIC CRYPTOGRAPHY

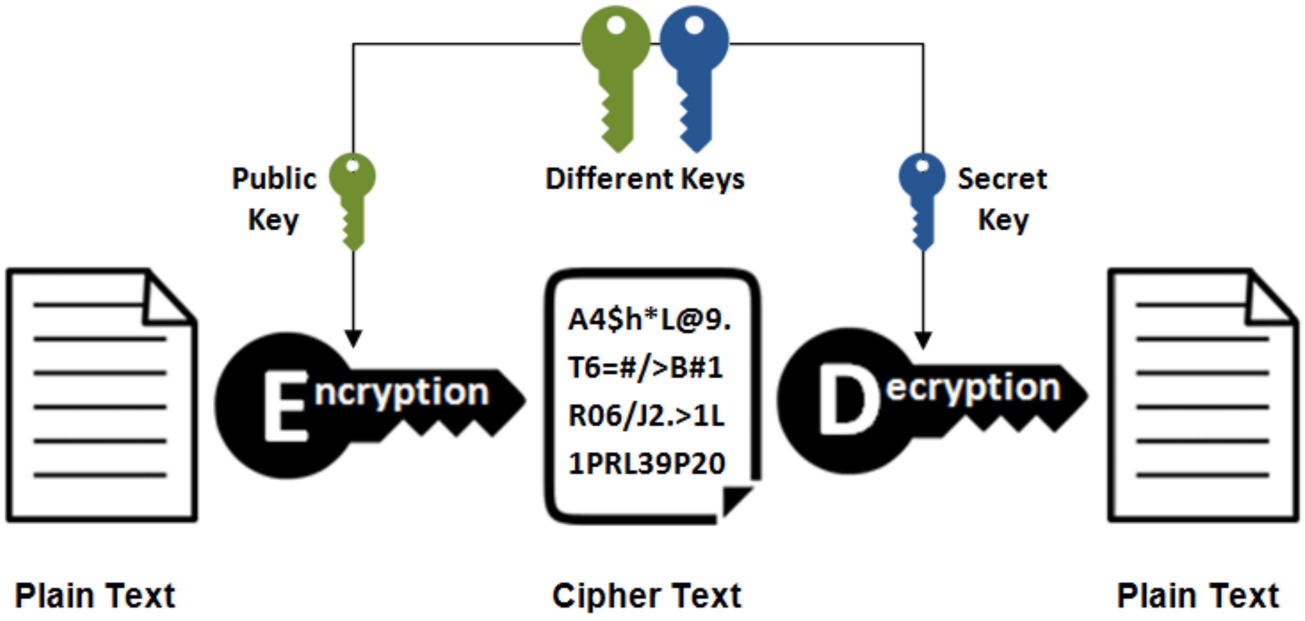
- Only **one secret key** for encryption and decryption
- Advantage
  - Fast
  - Small key size
- Disadvantage
  - Key establishment difficult
  - Only suitable for 1:1 communication
  - Group of n people → $\frac{n\,(n-1)}{2}$ keys
- Examples
  - DES, 3DES, AES



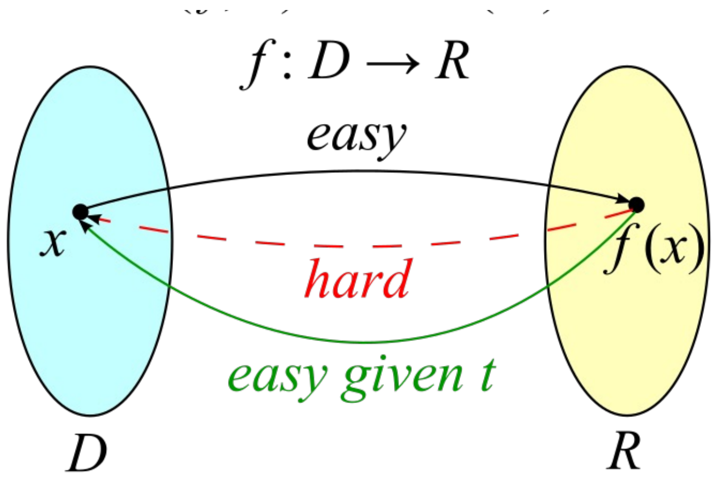
Source: https://en.wikipedia.org/wiki/Symmetric-key_algorithm

ASYMMETRIC CRYPTOGRAPHY

- On private/public key pair
- Advantage
  - Key establishment
  - Many-to-many communication
- Disadvantage
  - Large keys
  - Slow(er)
- Examples
  - RSA encryption (Rivest/Shamir/Adleman 1976)



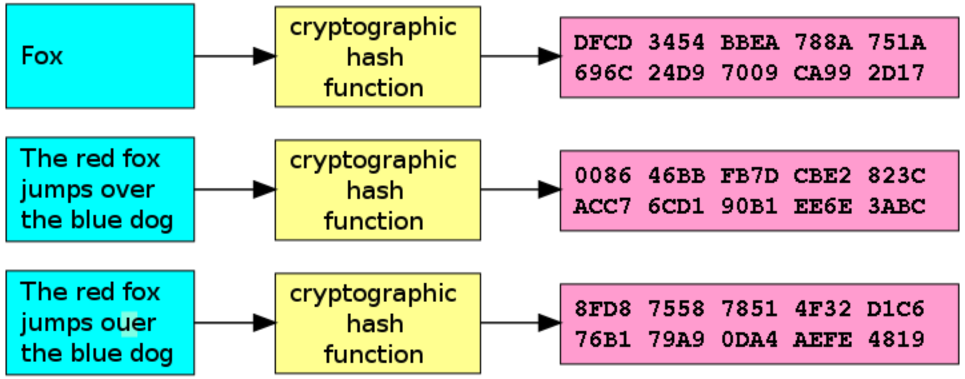
HASH FUNCTIONS



- Maps binary string to a binary string of fixed n bits
- One-way function
  - Calculating the hash is efficient
  - Finding an input string that matches a given hash value is unfeasible
  - Strong collision resistance

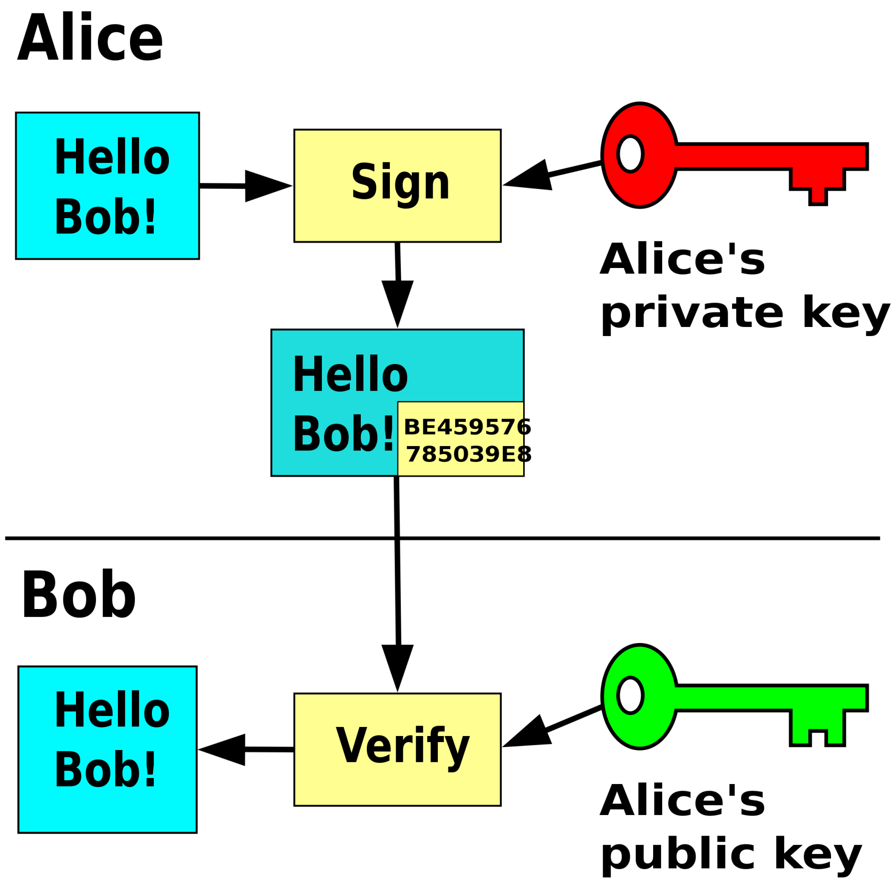
$$\text{hash}(m_1) = \text{hash}(m_2)$$

- Examples
  - ~~MD5~~, RIPEMD, SHA



DIGITAL SIGNATURES

- Digital Signatures for
  - Identification
  - Authenticity
  - Integrity
- Consists of
  - A public/private key pair
  - A signing algorithm
  - A verification algorithm.



Source: https://en.wikipedia.org/wiki/Public-key_cryptography

WHAT IS A BLOCKCHAIN?

WELL-KNOWN BLOCKCHAINS

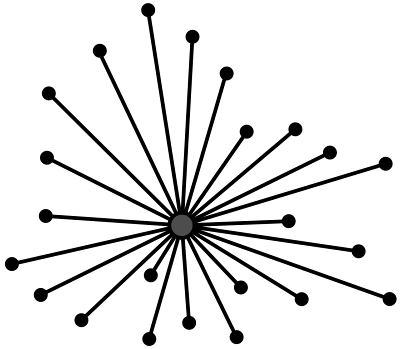
- Bitcoin (2008)
  - First Blockchain
  - Satoshi Nakamoto
  - Proof-of-Work
- Ethereum (2015)
  - Vitalik Buterin
  - Smart Contracts
  - Proof-of-~~Work~~ Stake

#	Name	Price	Market Cap	Volume(24h)	Circulating Supply
1	Bitcoin BTC	$40,064.02	$785,575,300,911	$19,673,951,270 490,867 BTC	19,608,000 BTC
2	Ethereum ETH	$2,224.71	$267,366,268,718	$9,006,694,391 4,046,938 ETH	120,180,143 ETH
3	Tether USDt USDT	$0.9996	$95,520,567,421	$34,804,844,468 34,824,358,284 USDT	95,554,092,991 USDT
4	BNB BNB	$291.16	$43,543,114,238	$953,460,216 3,270,281 BNB	149,548,056 BNB
5	Solana SOL	$87.58	$37,932,936,853	$1,982,038,699 22,571,199 SOL	433,135,580 SOL
6	XRP XRP	$0.5122	$27,834,002,697	$830,346,271 1,621,980,052 XRP	54,339,837,528 XRP
7	USDC USDC	$1.00	$25,853,581,595	$4,968,087,815 4,968,076,343 USDC	25,848,922,210 USDC
8	Cardano ADA	$0.4724	$16,729,544,876	$336,637,530 712,092,878 ADA	35,414,074,628 ADA

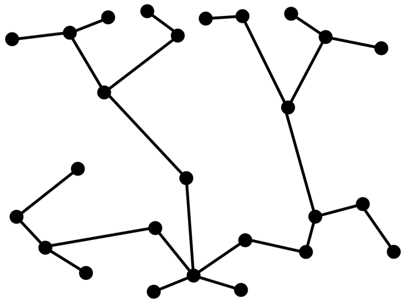
Screenshot CoinMarketCap from 2024/01/25

WHAT IS A BLOCKCHAIN

- Distributed and decentralized ledger system
- Every transaction is broadcasted to all users
- Miners collect transactions and create block
- Block records all transactions
  - Blocks are chained together via cryptography



CENTRALIZED



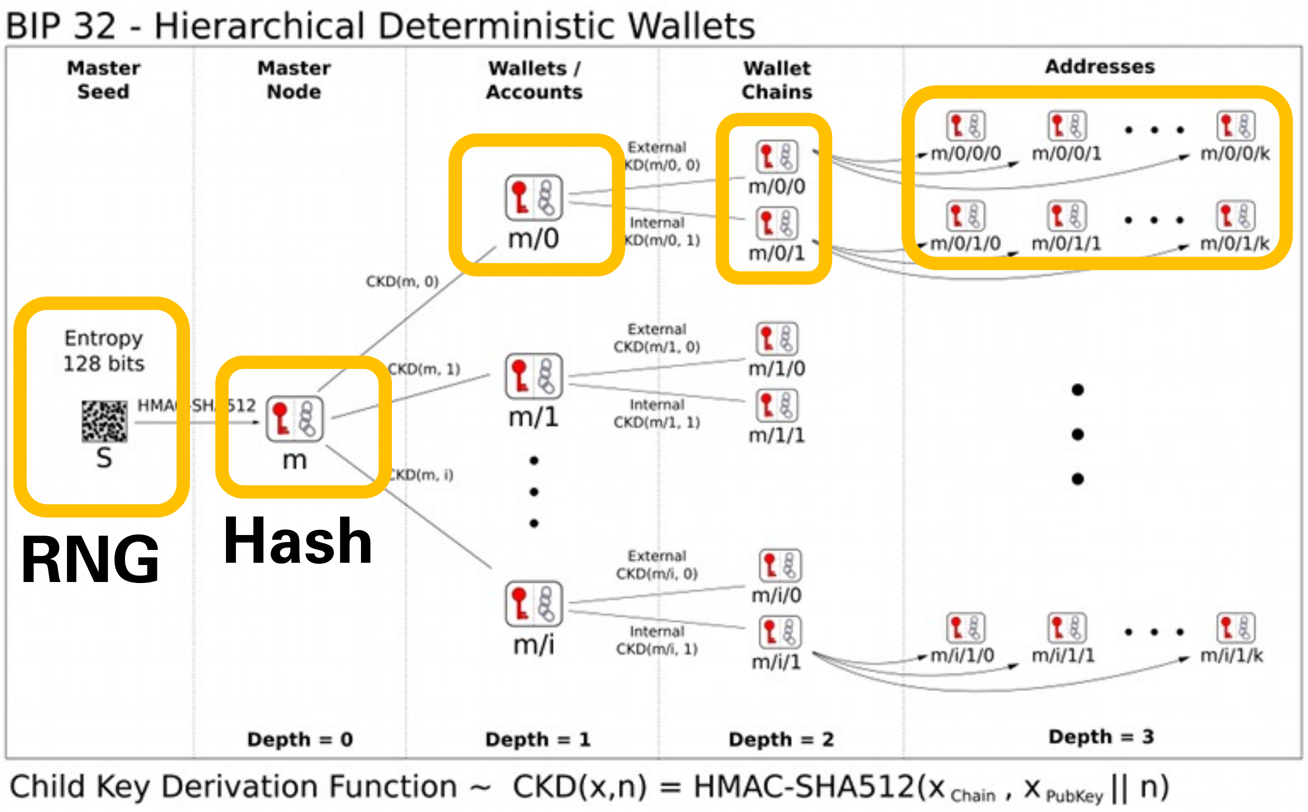
DECENTRALIZED

CHARACTERISTICS OF A BLOCKCHAIN

- Decentralization
  - Consensus algorithm
- Persistency (Immutability)
  - Once a block is created, a change of a transaction/block is (almost) impossible
  - Append only
- Anonymity / Pseudonymity
  - Public/private keys to identify users/accounts
- Auditability

KEY GENERATION

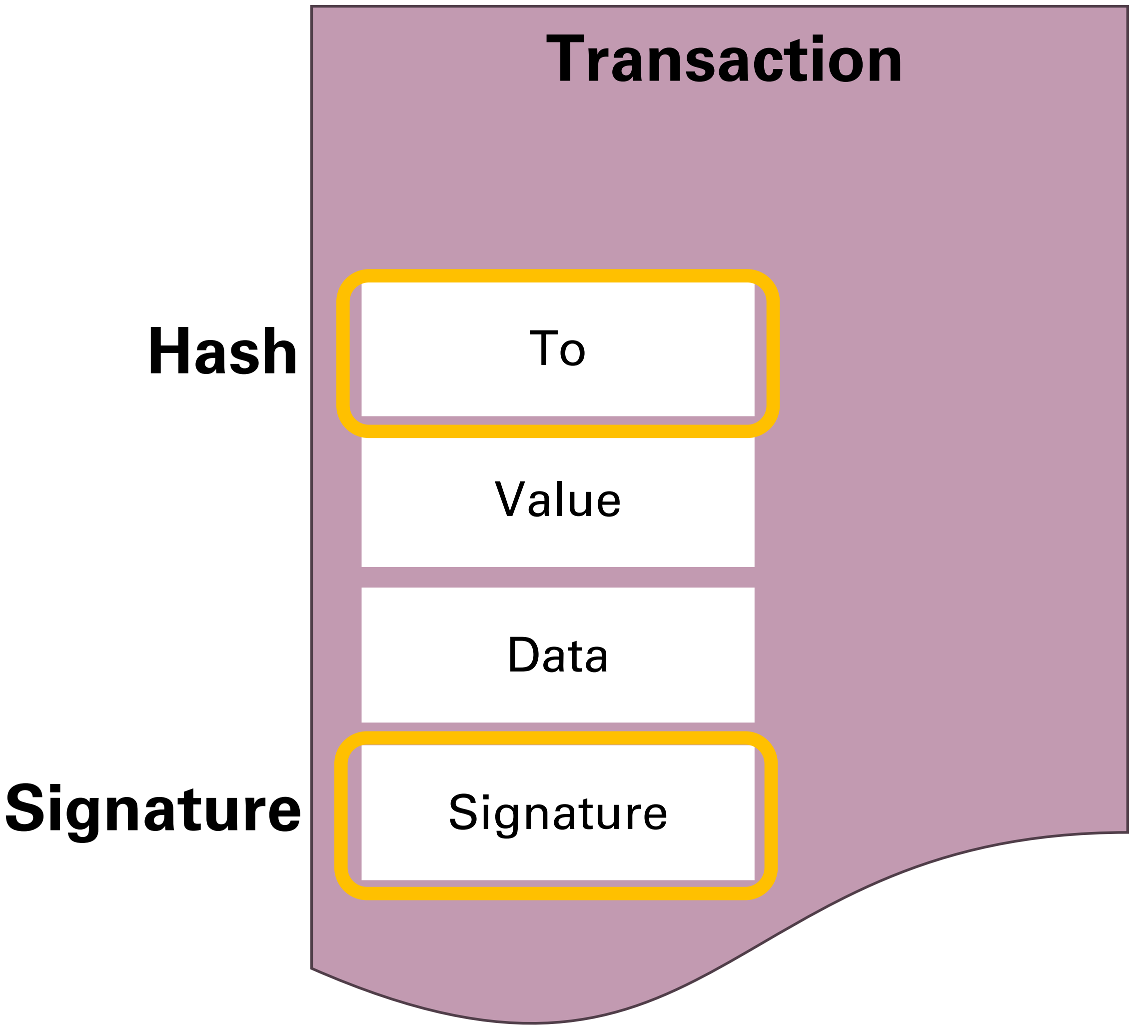
- Private key randomly generated
- Public address derived from private key
- Result of a bunch of hash calculations



Source: https://trezor.io/learn/a/what-is-bip32

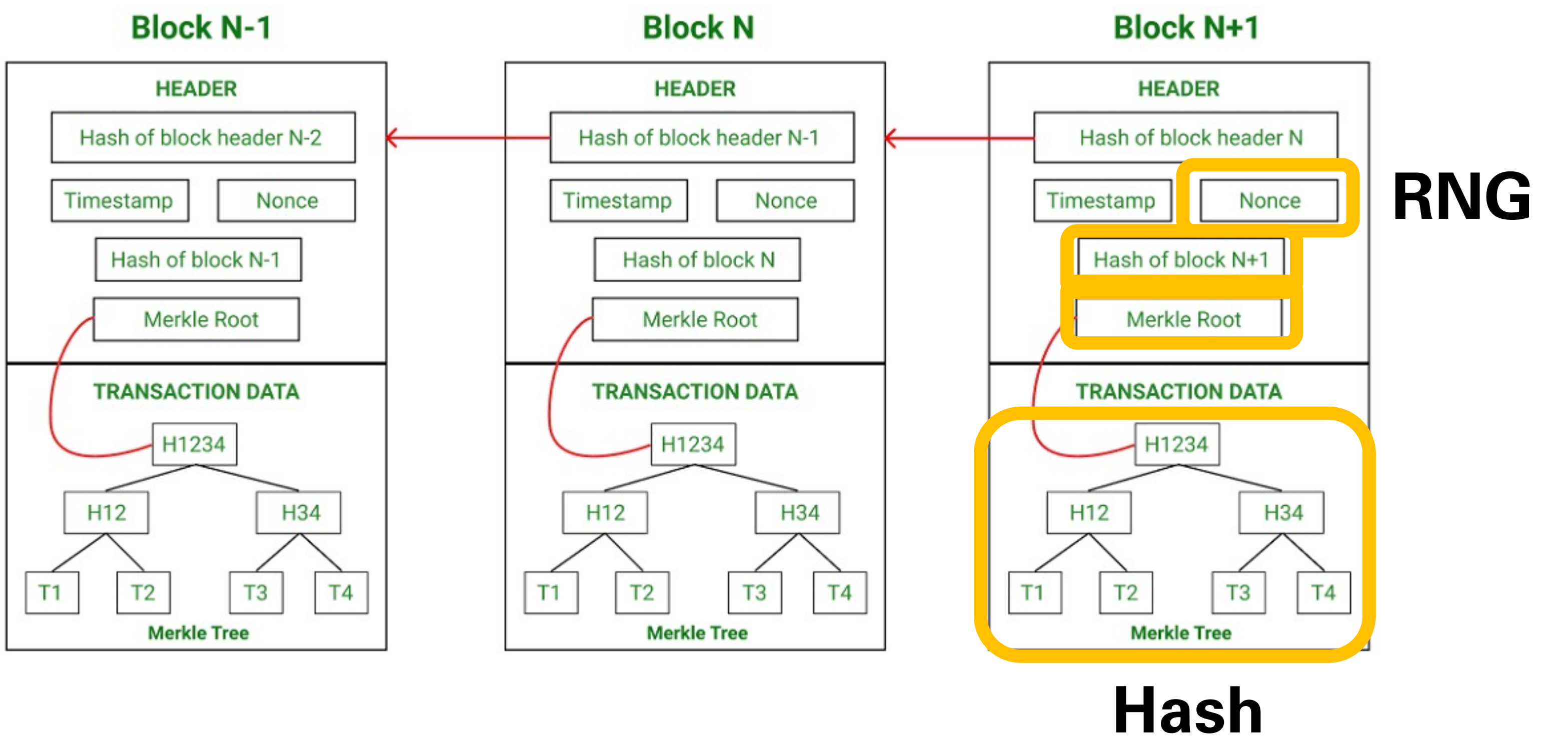
TRANSACTION

- Different types of transactions
  - Transfer/exchange of assets
  - Deployment of a smart contract
  - Execution of a smart contract
- Signed with private key
- Broadcasted to the network



BLOCKS

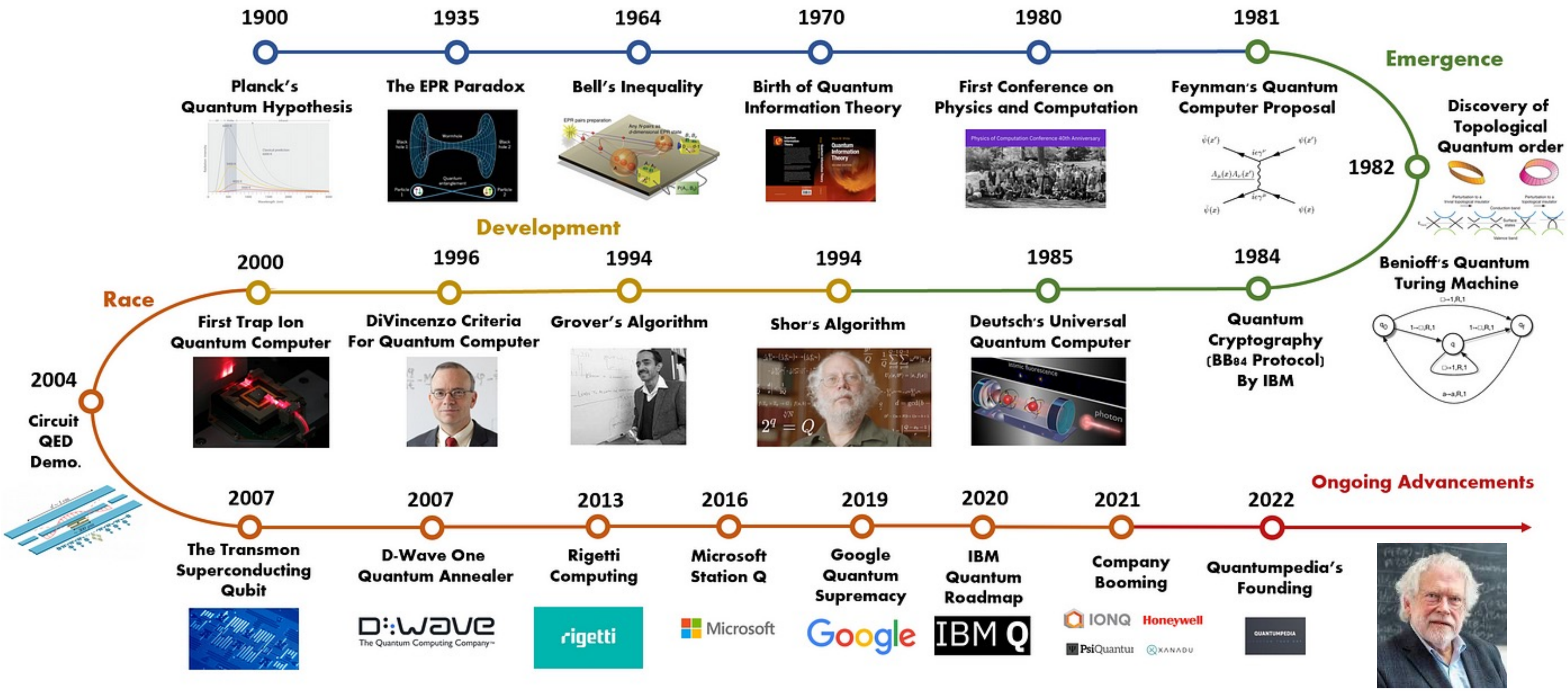
- Blocks
  - Records transactions
  - Timely ordered
- Consensus
  - In creating a block (e.g. POW)
  - In arranging blocks
  - In charge of verifying block
  - In ensuring everyone agrees on a block



Source: https://www.geeksforgeeks.org/blockchain-merkle-trees/

WHAT IS QUANTUM COMPUTING?

EVOLUTION OF QUANTUM TECHNOLOGY



QUANTUM TECHNOLOGIES

Sensing

Enhanced precision and sensitivity

- Atomic clocks
- Magnetometers for cavity detection
- MRI for brain scanners
- Quantum gravity-sensors for GPS assistance

Communication

Secure communication

- Random number generator
- Quantum Teleportation aka Quantum Internet
- Key distribution

Computing

Solving specific problems

- Quantum computing
- Cryptoanalysis
- Solving optimization problems
- Quantum machine learning
- Material science
- Monte Carlo, Portfolio

Further reading https://arxiv.org/pdf/2310.03011.pdf

THREE FUNDAMENTAL CONCEPTS

Superposition

the ability of a qubit to exist in **multiple states** simultaneously **until it is measured or observed**.

Interference

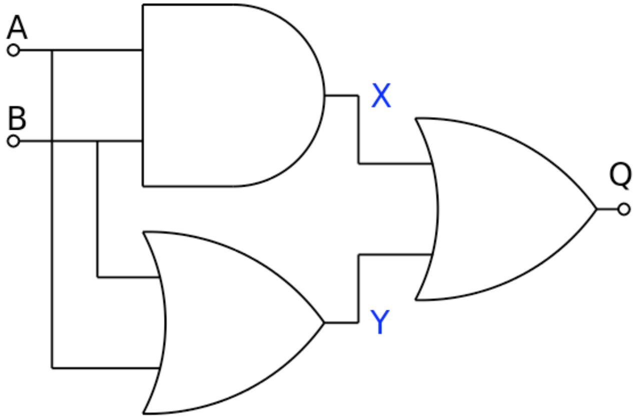
states can interfere with each other leading to **constructive** or **destructive** interference and interference can be used to **amplify certain outcomes and suppress others**.

Entanglement

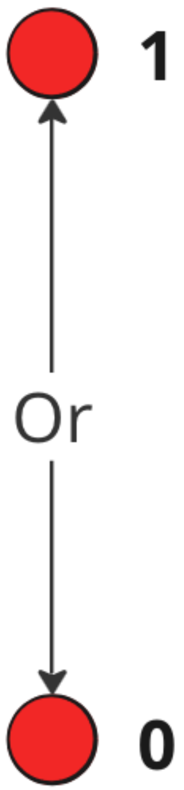
when two or more qubits become entangled, the properties of one qubit become **directly correlated** with the properties of another, **regardless of the distance** between them.

CLASSICAL COMPUTING

- The fundamental unit of information is the "bit".
- All classical computation is modifying bit sequences.
  - 1-bit operations like SET and NOT
  - 2-bit operations like AND, OR, XOR

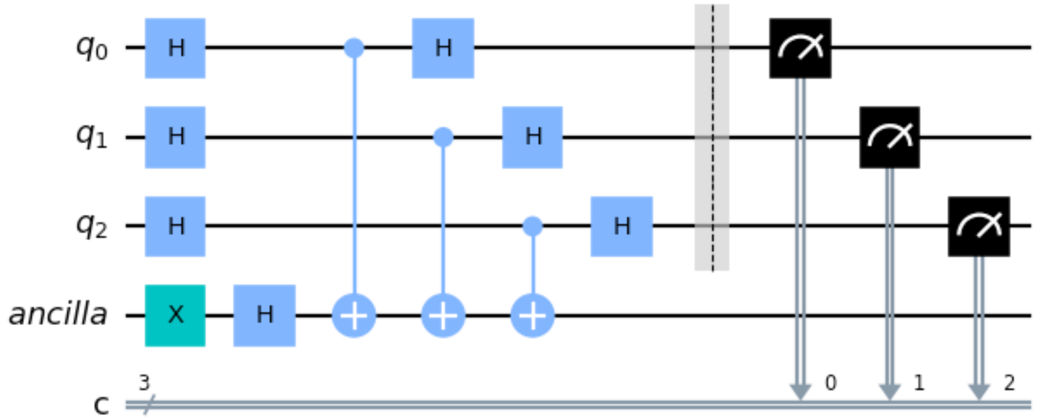


A	B	X	Y	Q
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	1

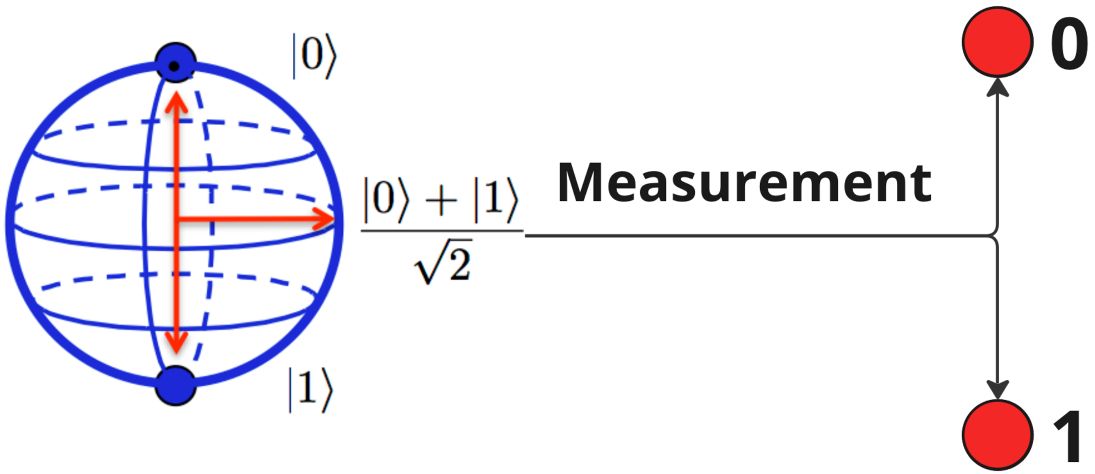


Classical Bit

QUANTUM COMPUTING



- The fundamental unit of information is the "qubit".
- Qubits are in a **superposition** of $a\,|0\rangle + b\,|1\rangle$
  - With *a* and *b* being complex numbers
- Qubits can be **entangled**
- Qubits can be **manipulated** by gates
- Observing (**measuring**) a qubit turns it into a classical 0 or 1

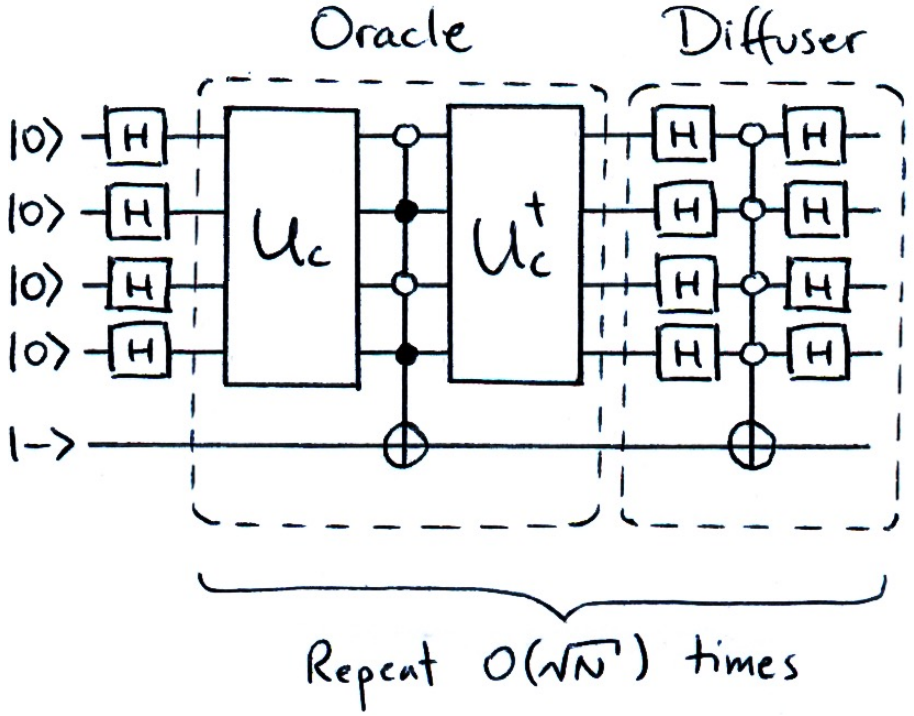


QUANTUM SPECIFIC ALGORITHMS

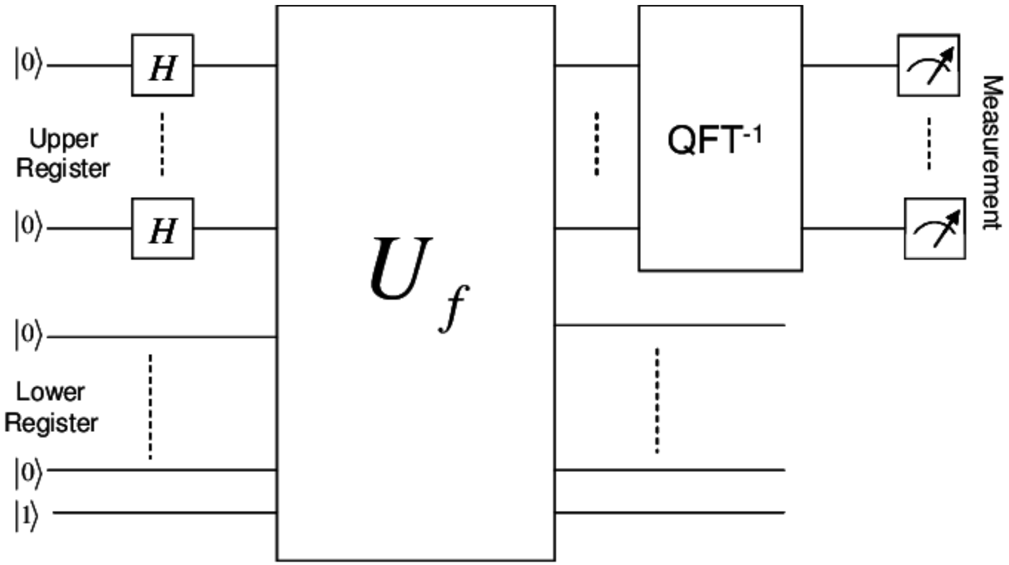
- Variational Quantum Algorithms (VQA)
- Quantum Approximate Optimisation Algorithms (QAOA)
- Quadratic Unconstrained Binary Optimization (QUBO)
- Deutsch-Jozsa-Algorithm
- Grover’s Algorithm
- Shor’s Algorithm

GROVER'S ALGORITHM

- Developed by Lov Grover in 1994
- **Search** for an element in an **unsorted set** that satisfy one or more conditions (Oracle)
- Classically N evaluations in worst case
- Grover solves this problem using O(√(N))



SHOR'S ALGORITHM

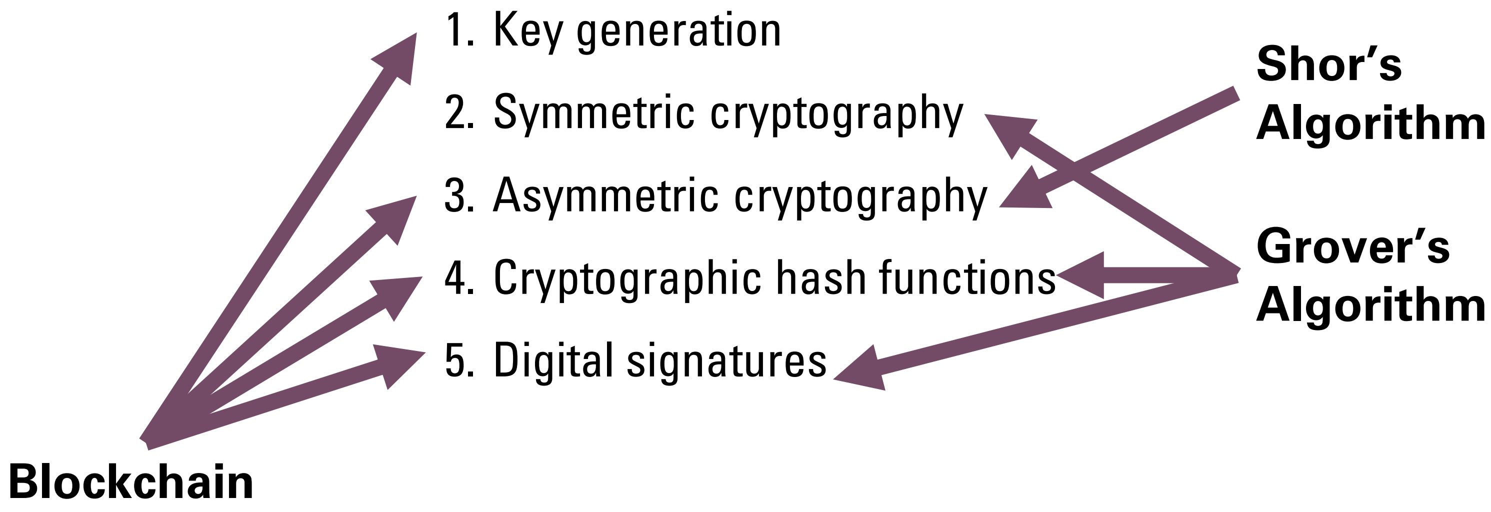


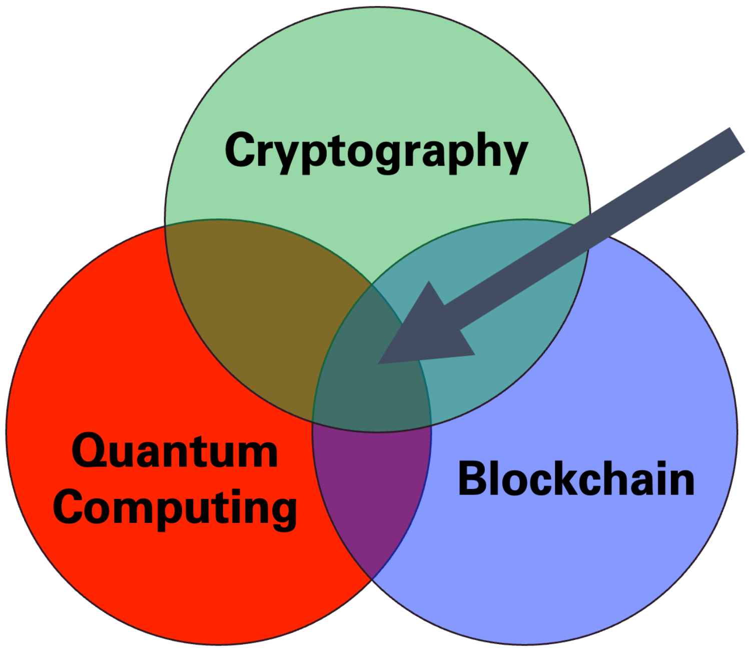
- Developed by Peter Shor in 1994
- **Factorisation of huge integers**
  1 < p, q < N and n = pq
    - 21 = [redacted]
    - 52.866.631 = [redacted]
    - 2211282552952966643528108525502623092761208950247001539441374831912882294140200198651272972656974659908590033003140005117074220456085927635795375718595498838958709229238491006703034124620545784566413664540684214361293017694020846391065875914794251435144458199 = [redacted]
      https://en.wikipedia.org/wiki/RSA_numbers#RSA-260 (862 bits!)
- A lot of cryptographic systems base their security on **computationally hard problems**
- Speedup compared to classical algorithms is still very high even if run several times.

THREATS TO BLOCKCHAIN

Let’s put the things together…

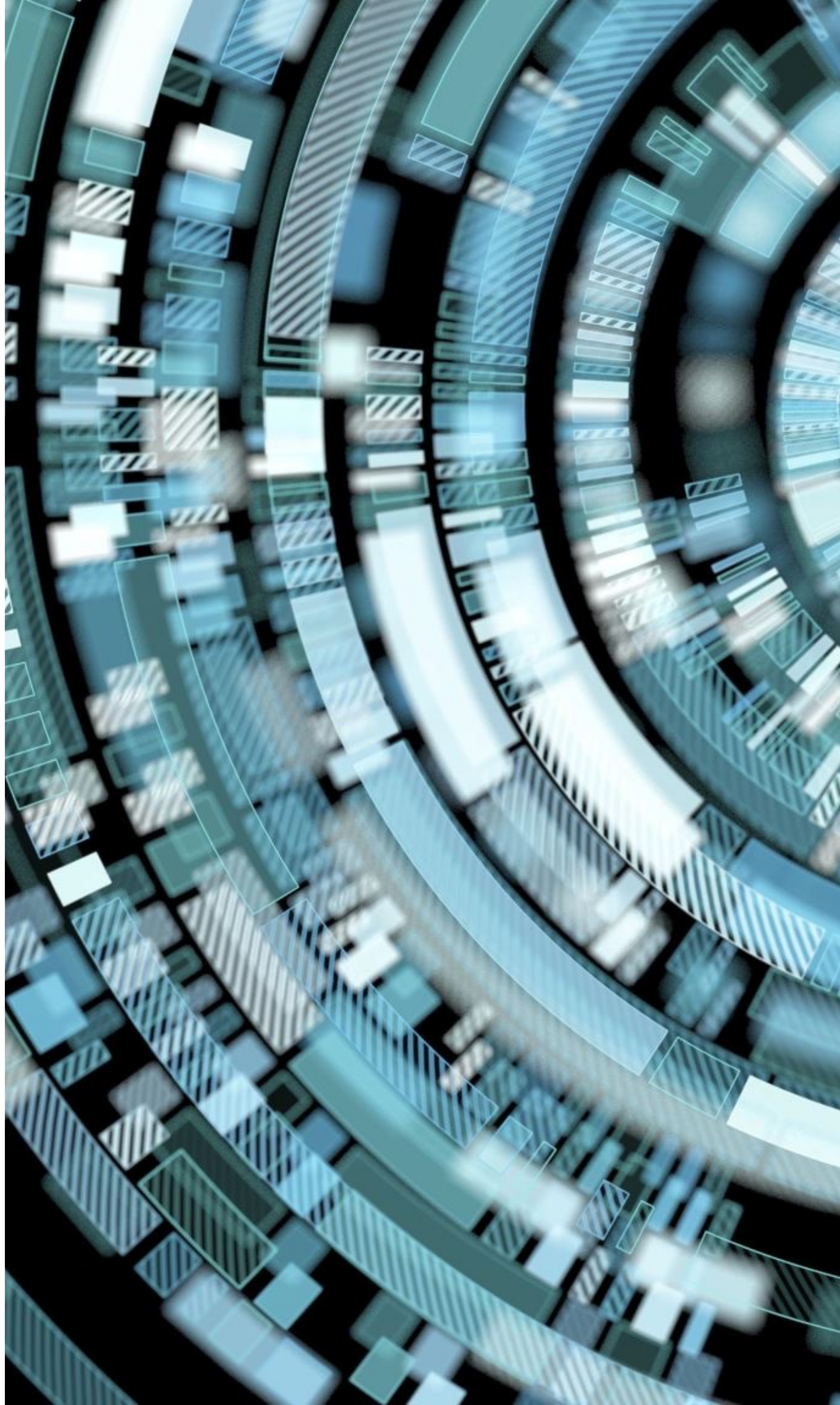
COMPONENTS OF A CRYPTOSYSTEM





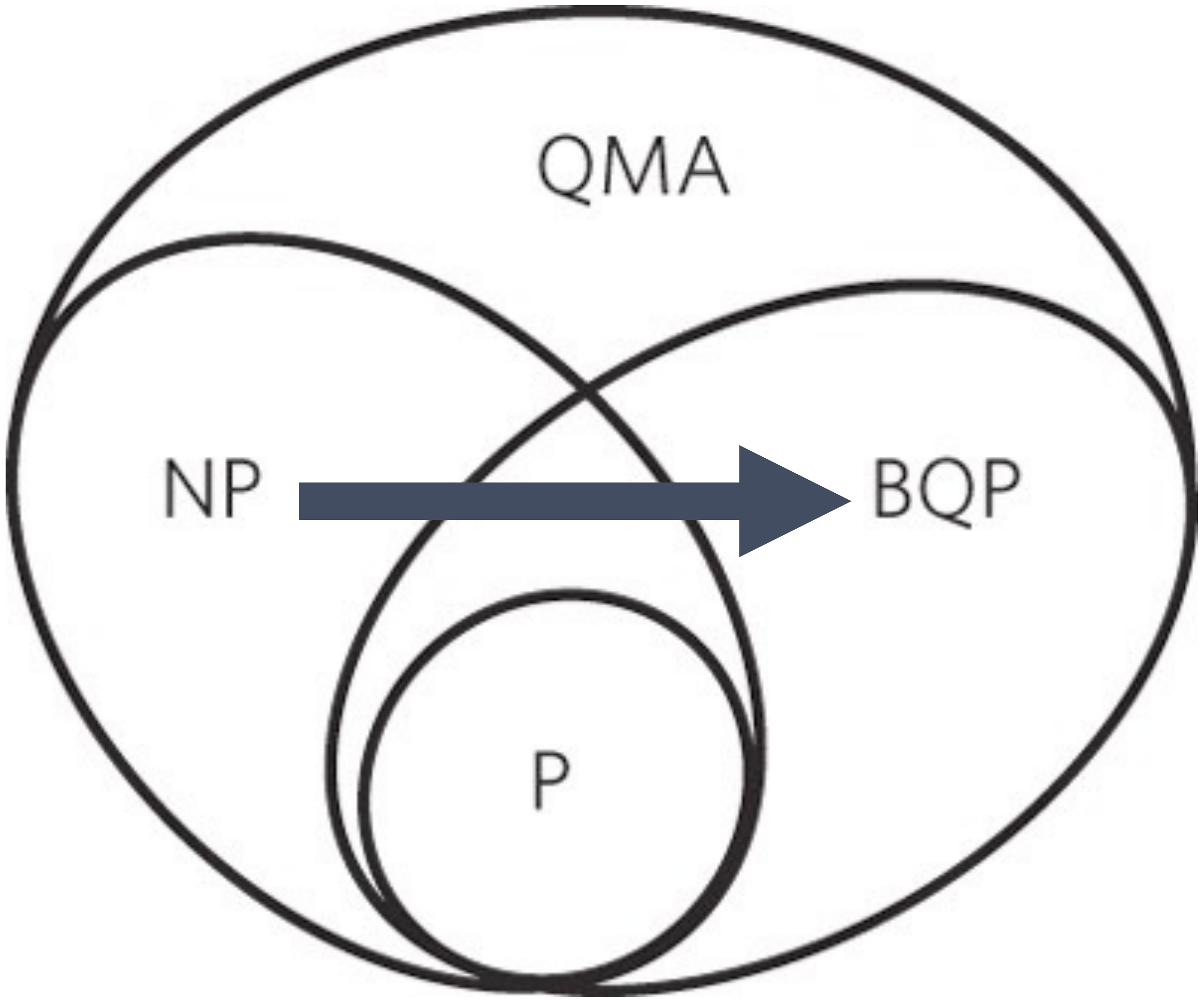
MINING PROTOCOL

- Problem
  - POW is a NP-hard problem
    - Grover's Algorithm
  - Possible attacks to POW consensus by computational advantage of QC
    - 51% attack
    - Stale blocks generation
    - High stale rate (less than 50% attack!)



REPLACE / UPGRADE CONSENSUS

- Changing from POW to POx
    - Consensus mechanisms like POS or DPOS which don't rely on computing power
- Improved POW algorithms without quantum advantage
    - Replacing crypto functions with quantum-safe ones



HASHING FUNCTIONS

- Problem
  - Attacks on signatures
    - The signature of that transaction reveals the public key
    - Finding the private key (Grover's Algorithm)
  - Processed transactions
    - UTXO
    - Long time: Some transactions are "old"
  - Unprocessed transactions
    - Transaction front-running
    - Fast: Only time to next block

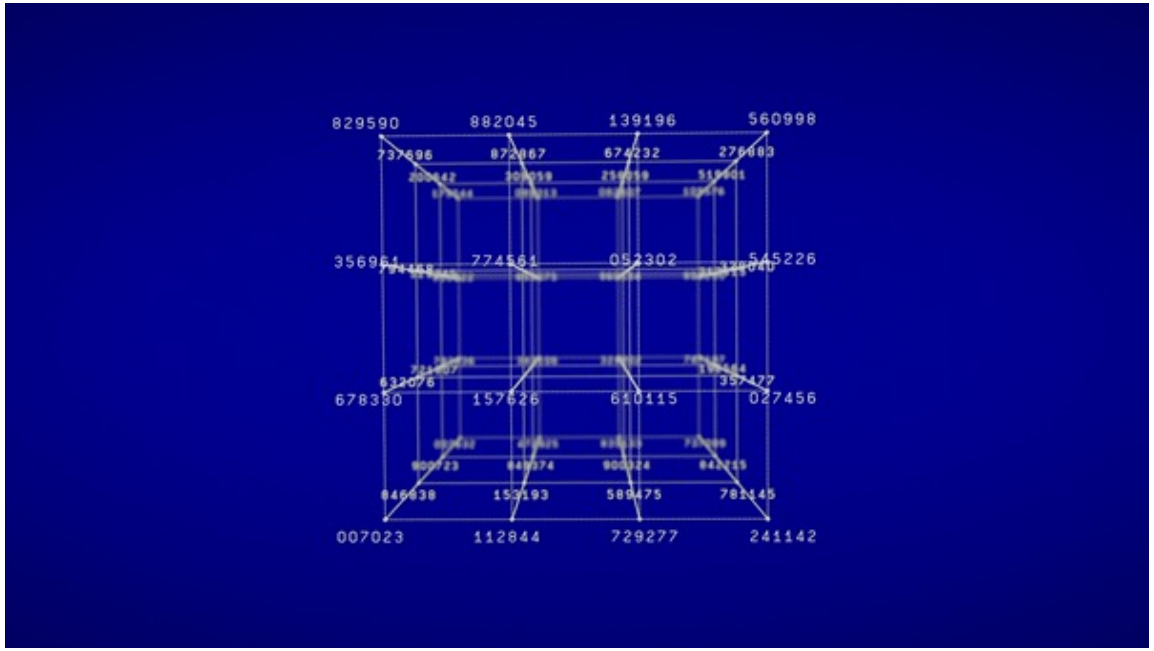
QUANTUM AVAILABILITY

- Size:
  - Largest quantum chip of IBM has 1,121 physical qubits
- Speed:
  - QCs are slow by clock frequency
  - Preparation/readout of circuits takes long

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required[a]	Time Required to Break System[b]	Quantum-Resilient Replacement Strategies
AES-GCM[c]	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} years 1.97×10^{22} years 2.29×10^{32} years	
RSA[d]	Asymmetric encryption	1024 2048 4096	80 112 128	Shor's algorithm	2,050 4,098 8,194	8.05×10^6 8.56×10^6 1.12×10^7	3.58 hours 28.63 hours 229 hours	Move to NIST-selected PQC algorithm when available
ECC Discrete-log problem[e-g]	Asymmetric encryption	256 384 521	128 192 256	Shor's algorithm	2,330 3,484 4,719	8.56×10^6 9.05×10^6 1.13×10^6	10.5 hours 37.67 hours 55 hours	Move to NIST-selected PQC algorithm when available
SHA256[h]	Bitcoin mining	N/A	72	Grover's Algorithm	2,403	2.23×10^6	1.8×10^4 years	
PBKDF2 with 10,000 iterations[i]	Password hashing	N/A	66	Grover's algorithm	2,403	2.23×10^6	2.3×10^7 years	Move away from password-based authentication

ALTERNATIVE CRYPTO SCHEMES

- Code-Based Cryptosystems
- Hash-Based Cryptosystems
- Multivariate Cryptosystems
- Lattice-Based Cryptosystems
  - Shortest Vector Problem (SVP)
  - Closest Vector Problem (CVP)
  - Shortest Independent Vectors Problem



NIST PQC COMPETITION

- PQC: Post Quantum Cryptography
- For applications TLS, SSH, IPsec, DNSSEC,...
- NIST PQC competition on-going (since 2016!)
  - https://csrc.nist.gov/projects/post-quantum-cryptography
- Public-key Encryption and Key-establishment Algorithms
  - CRYSTALS-KYBER (FIPS 203 – ML-KEM)
- Digital Signature Algorithms
  - CRYSTALS-DILITHIUM (lattice) (FIPS 204 – ML-DSA)
  - FALCON (lattice)
  - SPHINCS+ (hash) (FIPS 205 - SLH-DSA)

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

PROBLEM: SIZES OF KEYS AND SIGNATURES

	Falcon-512	Falcon-1024
Target NIST Level	I	V
Ring degree n	512	1024
Modulus q	12289	
Standard deviation σ	165.736 617 183	168.388 571 447
$\sigma_{\min}$	1.277 833 697	1.298 280 334
$\sigma_{\max}$	1.8205	
Max. signature square norm $\lfloor \beta^2 \rfloor$	34 034 726	70 265 242
Public key bytelength	897	1 793
Signature bytelength sbytelen	666	1 280

~ RSA-2048
(256 bytes each)

Dilithium5

Sizes (in bytes)		Skylake cycles (ref)		Skylake cycles (avx2)	
sk:		gen:	819475	gen:	298050
pk:	2592	sign:	2856803	sign:	642192
sig:	4595	verify:	871609	verify:	279936

Type	Public key size (B)	Secret key size (B)	Ciphertext size (B)
Kyber512	800	1,632	768
Kyber738	1,184	2,400	1,088
Kyber1024	1,568	3,168	1,568
LightSABER	672	1,568	736
SABER	992	2,304	1,088
FireSABER	1,312	3,040	1,472
McEliece348864	261,120	6,452	128
McEliece460896	524,160	13,568	188
McEliece6688128	1,044,992	13,892	240
McEliece6960119	1,047,319	13,948	226
McEliece8192128	1,357,824	14,120	240
NTRUhps2048509	699	935	699
NTRUhps2048677	930	1,234	930
NTRUhps4096821	1,230	1,590	1,230

~ AES-256
(32 bytes)

KEY GENERATION / EXCHANGE

- Problem
  - Weakness in randomness
    - Pseudo random number generation (PRNG)
    - Low entropy on system
    - Buggy implementation
  - Plaintext transmission
    - Intercepting communication

coinlive.com

Klever Wallet: All affected wallets are imported after being generated using the pseudo-random number generator algorithm. Users are advised to create new wallets

Klever Created by Wallet K5, all wallets are generated and imported into Klever Wallet K5, and are created using the old, weak pseudo-random number generator PRNG algorithm as an entropy source, which will seriously damage the security and unpredictability of private key generation. Thus, it may be more

https://www.coinlive.com/news-flash/24467 (13/07/2023)

QUANTUM RANDOMNESS

- Quantum Random Number Generators (QRNG)
  - Using quantum mechanics
- Real randomness is intrinsic property of quantum mechanics
- QRNGs
  - Available for normal use
  - No longer limited by speed (> 250 Kbps)
  - Daily use (IPSEC, HTTPS, SSH, Simulations,...)

https://www.idquantique.com/random-number-generation/qrng-use-cases/samsung-qrng-use-case/

QUANTUM KEY DISTRIBUTION

- Quantum Internet
  - Quantum teleportation to create tap-prof channel
  - Using QKD to exchange keys to secure transactions
  - Needs new infrastructure

SOME FURTHER READING

- Quantum solutions to possible challenges of Blockchain technology
  arXiv:2110.05321v1 [cs.CR] 11 Oct 2021
- Conditions for Advantageous Quantum Bitcoin Mining
  arXiv:2110.00878v1 [quant-ph] 2 Oct 2021
- On the insecurity of quantum Bitcoin mining
  arXiv:1804.08118v4 [quant-ph] 12 Feb 2019
- Quantum attacks on Bitcoin, and how to protect against them
  arXiv:1710.10377v1 [quant-ph] 28 Oct 2017
- Strategies for quantum races
  arXiv:1809.03671v2 [quant-ph] 27 Sep 2018
- Quantum Computing: Progress and Prospects
  The National Academies Press. https://doi.org/10.17226/25196.
- Introducing Quantum Secured Blockchain: A Comprehensive Whitepaper
  https://www.quantumblockchains.io/introducing-quantum-secured-blockchain-a-comprehensive-whitepaper/
- Architecture for Blockchain Applications
  Springer; 1st ed. 2019 edition (March 15, 2019)
- Bit Commitment for Lottery and Auction on Quantum
  Blockchainhttps://arxiv.org/abs/2004.10312
- Quantum Attacks on Bitcoin, and How to Protect Against Them
  https://ledgerjournal.org/ojs/index.php/ledger/article/view/127
- Quantum-secured blockchain
  https://stacks.iop.org/2058-9565/3/i=3/a=035004
  https://arxiv.org/abs/1705.09258
- Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic
  https://www.mdpi.com/1099-4300/21/9/887
- An Overview of Hash Based Signatures
  https://eprint.iacr.org/2023/411.pdf
- Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic
  https://www.mdpi.com/1099-4300/21/9/887
- Quantum Resistant Ledger (QRL)
  https://github.com/theQRL/Whitepaper/blob/master/QRL_whitepaper.pdf

QUANTUM-FIRST BLOCKCHAINS

A QUANTUM-FIRST BLOCKCHAIN

Utilising QT for improving security of blockchain.

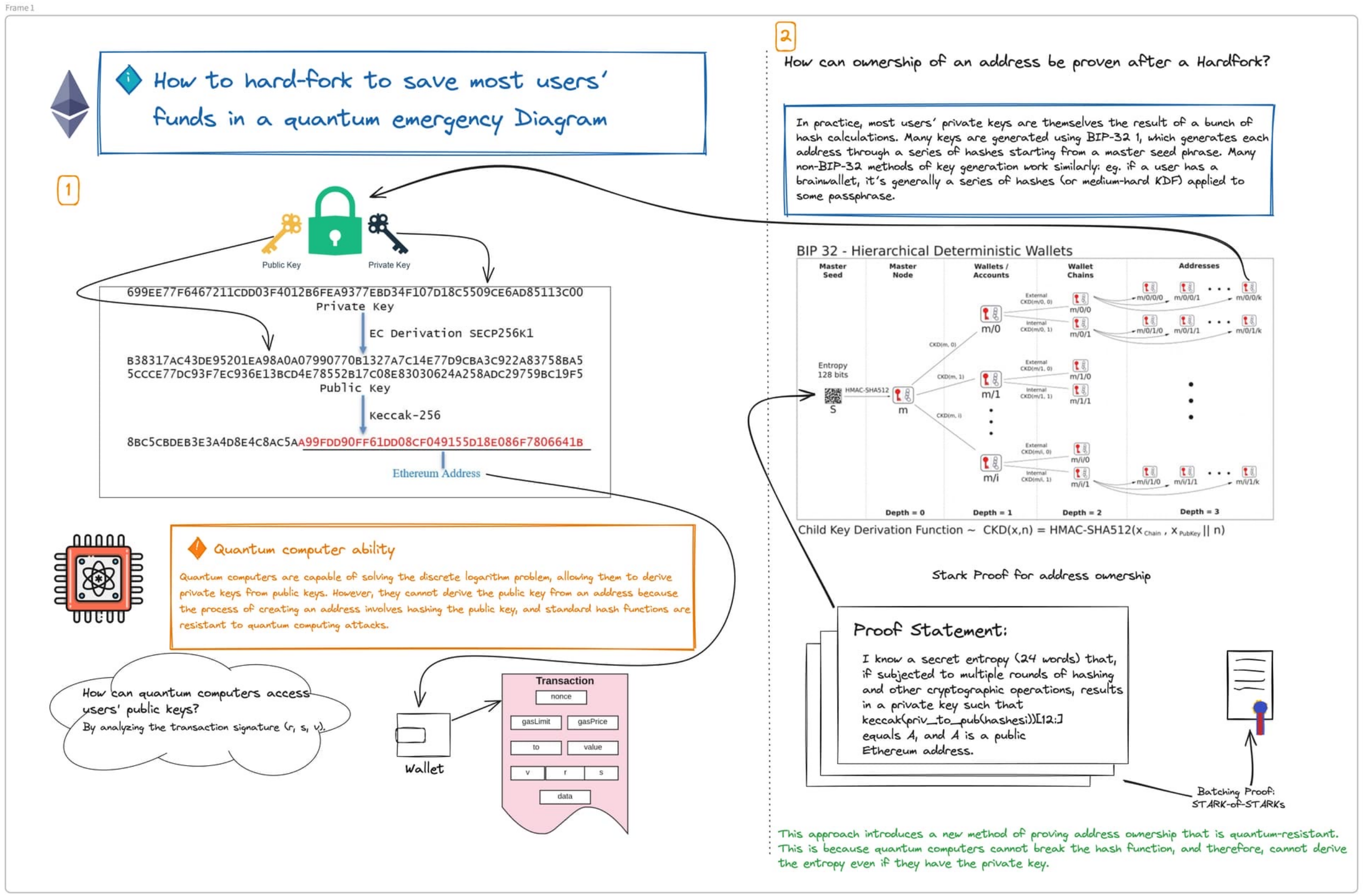
- Random Number Generation
  - Improved key generation
  - Randomness for nonce
- Enhanced Computational Power
  - Quantum Smart Contracts
- Post Quantum Cryptography
  - Secure Internode Communication (QKD)
- Improved Consensus Mechanisms
  - Quantum Resistant Algorithms

OBSTACLES TO QUANTUM-FIRST BLOCKCHAIN

- Limited Availability of Quantum Computing Resources
- Paradigm Shift in Programming
- Designing Quantum Algorithms
- Quantum Error Correction
- Integration with Classical Systems
- Lack of Standardization
- Speed and memory usage for the ‘verify’ operation
- Key and signature size
- Incompatibility with existing hardware
- Network effect
- Missing community
- …

ETHEREUM

- https://ethereum.org/
- POS
- Transactions still “vulnerable”
- Post by Vitalik suggesting hard-fork
  - Winternitz signatures
  - STARKs
  - Account Abstraction



https://ethresear.ch/t/how-to-hard-fork-to-save-most-users-funds-in-a-quantum-emergency/18901

QRL - THE QUANTUM RESISTANT LEDGER

- https://www.theqrl.org/
- XMMS
  - https://datatracker.ietf.org/doc/html/rfc8391
  - https://csrc.nist.gov/pubs/sp/800/208/final (recommendation)
  - WOTS+ - Winternitz scheme
- QRL enQlave Project – “Bringing Post-Quantum Security to Ethereum”
- Beta-Testnet on 15th January

Visionary Security

QRL is the first industrial implementation to utilize IETF specified XMSS; a hash-based, forward secure signature scheme with minimal security assumptions and reusable addresses.

QRL: The Quantum Resistant Ledger
@QRLedger

After months of dedication, development, and collaboration, we are delighted to unveil the official launch date for our public beta-testnet v1: January 15th, 2024!

As we unveil the entrance to our public beta-testnet v1 from devnet, developers across the globe are invited to delve into and interact with our platform and ecosystem...

This encompasses web3 and EVM smart contract capabilities, all built upon a post-quantum secure foundation. Those with experience in the Ethereum ecosystem will find themselves right at home in this innovative environment.

In this developmental phase, as we refine nodes and work towards public beta-testnet v2 (with additional improvements & incorporating a new address format), there is a prime opportunity to construct essential ecosystem components. This includes the development of wallets, explorers, and various tools that will enhance the overall functionality and user experience within our platform.

More details will be shared through documentation and other media channels as the release date gets closer 💻🔐📅

5:35 PM · Dec 21, 2023 · **2,826** Views

EnQlave: Quantum Security for Ethereum

EnQlave is an education initiative and ecosystem which brings **trustless on-chain post-quantum security** (the EnQlave wallet) and **cross-chain interoperability with QRL** (wQRL + DEX) to sufficiently scriptable and supported blockchains, starting with Ethereum.

CARDANO

https://cardano.org

Cardano's Proactive Approach to Quantum Computing: Ensuring a Secure Future

SourceDao · Follow
2 min read · May 5

Integrating Quantum-Resistant Cryptography

In response to the potential threat of quantum computing, Cardano is exploring the integration of quantum-resistant cryptographic algorithms into its blockchain. These post-quantum algorithms are designed to withstand attacks from quantum computers, ensuring the security of the network and its users. By incorporating these algorithms, Cardano can better protect itself from the risks associated with quantum computing advancements.

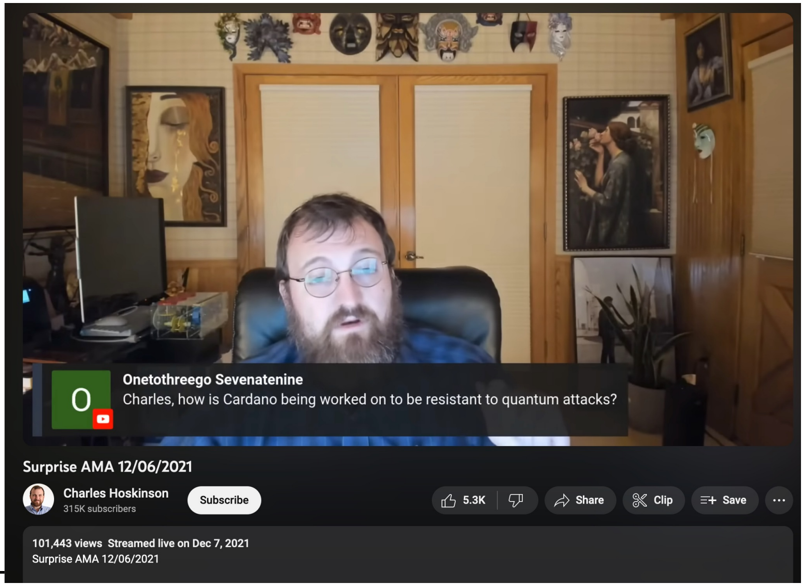
May 5, 2023

Why Cardano

Introduction

For Cardano, we decided to start with using elliptic curve cryptography, the Ed25519 curve in particular. We also decided to enhance the existing libraries by adding support for HD wallets using Dr Dmitry Khovratovich and Jason Law's Specification[8].

This said, Cardano will support more signature schemes in the future. In particular, we are interested in integrating quantum computer resistant signatures to our system.



LACCHAIN

- https://www.lacchain.net/
- Falcon-512 NIST-compliant post-quantum signatures
- EVM-compatible
- Tackling on many layers
    - Quantum secure communication
    - QKD
    - PQC
    - PoA mining

QANPLATFORM

- https://www.qanplatform.com
- EVM-Compatible
- Multi-language Smart Contracts aka Hyperpolyglot
- Proof-of-Randomness (PoR)
  - “highly experimental concept that requires extensive technological and economic modeling, testing, and auditing”
- Lattice-based post-quantum cryptographic

	QANplatform	Bitcoin	Ethereum
Transaction speed	private: 95,000 tps public: 1,600< tps	7 tps	14 tps
Decentralization level	3/3	3/3	2/3
Programming language	any language	no	Solidity
Consensus algorithm	PoR	PoW	PoW
Hybrid blockchain	yes	no	yes
Ethereum EVM compatibility	yes	no	yes
Cloud deployment time	5 minutes	-	hours
Quantum-resistant security	yes	no	no
Market cap (in USD)	$103M	$1,089B	$515B

MOCHIMO

https://mochimo.org/

PERSPECTIVES…

NOT DOOMED! AT LEAST NOT NOW!

Not all cryptocurrencies are (equally) vulnerable

Solutions discussed or implemented

- Employing PQC algorithms
- Proof of Stake

We still have time...

→ Quantum computers are not powerful enough before 2030 (or at all!)